



คู่มือผู้ใช้ HP Sure Admin

สรุป

HP Sure Admin ช่วยให้ผู้ดูแลระบบ IT สามารถจัดการการตั้งค่าเฟิร์มแวร์ของอุปกรณ์ที่สำคัญได้อย่างปลอดภัย โดยใช้ไมรับรองและการเข้ารหัสคีย์สาธารณะ เพื่อจัดการการตั้งค่าทั้งแบบระยะไกลและแบบโลคัลแทนการใช้อีพียูผ่าน

ข้อมูลทางกฎหมาย

© Copyright 2019, 2021 HP Development Company, L.P.

Apple เป็นเครื่องหมายการค้าของ Apple Computer, Inc. ซึ่งจดทะเบียนในสหรัฐอเมริกาและประเทศอื่น ๆ

Google Play เป็นเครื่องหมายการค้าของ Google LLC

ซอฟต์แวร์คอมพิวเตอร์ลิขสิทธิ์เฉพาะ ต้องได้รับการอนุญาตอย่างถูกต้องจาก HP สำหรับการครอบครอง ใช้ หรือคัดลอก ตามระเบียบของ FAR มาตรา 12.211 และ 12.212 ได้ให้การอนุญาตใช้ซอฟต์แวร์คอมพิวเตอร์เพื่อการพาณิชย์ เอกสารประกอบซอฟต์แวร์คอมพิวเตอร์ และข้อมูลทางด้านเทคนิค กับรัฐบาลสหรัฐอเมริกา ภายใต้การอนุญาตใช้เชิงพาณิชย์ตามมาตรฐานของผู้ค้า

ข้อมูลที่เราไว้ในที่นี้อาจมีการเปลี่ยนแปลงได้โดยไม่ต้องแจ้งให้ทราบล่วงหน้า ทั้งนี้การรับประกันสำหรับผลิตภัณฑ์และบริการของ HP จะเป็นไปตามข้อกำหนดการรับประกันโดยชัดแจ้งซึ่งแนบมาพร้อมกับผลิตภัณฑ์และบริการดังกล่าวเท่านั้น ข้อความในที่นี้จะไม่ส่งผลในการรับประกันเพิ่มเติมใดๆ ทั้งสิ้น โดย HP จะไม่รับผิดชอบต่อข้อผิดพลาดหรือการตกหล่นของข้อมูลทางเทคนิคหรือของเนื้อหาในเอกสารนี้

พิมพ์ครั้งที่สอง: ตุลาคม 2021

พิมพ์ครั้งที่หนึ่ง: ธันวาคม 2019

หมายเลขชิ้นส่วนของเอกสาร: L83995-282

สารบัญ

| | |
|--|----------|
| 1 การเริ่มต้นใช้งาน | 1 |
| การใช้ HP Sure Admin | 1 |
| การปิดใช้งาน HP Sure Admin | 1 |
| 2 การสร้างและการจัดการคีย์ | 2 |
| การสร้างและการส่งออกคีย์ | 2 |
| สร้างและส่งออกคีย์โดยวิธีการกระจายด้วยตนเอง | 2 |
| การสร้างและส่งออกคีย์ด้วย Azure AD Revocation..... | 3 |
| สร้างและส่งออกคีย์ไปยัง Azure AD Group OneDrive | 4 |
| 3 การตั้งค่าโทรศัพท์..... | 5 |
| การใช้แอปโทรศัพท์ HP Sure Admin เพื่อปลดล็อก BIOS..... | 5 |
| การขอรับสิทธิ์เข้าถึงการตั้งค่า BIOS หลังการลงทะเบียน..... | 5 |
| การปลดล็อก BIOS ด้วย Azure AD Group OneDrive | 6 |
| 4 รหัสข้อผิดพลาดของ HP Sure Admin | 7 |

1 การเริ่มต้นใช้งาน

HP Sure Admin ช่วยให้ผู้ดูแลระบบ IT สามารถจัดการการตั้งค่าเฟิร์มแวร์ของอุปกรณ์ที่สำคัญได้อย่างปลอดภัย โดยใช้โมบายรอง และการเข้ารหัสคีย์สาธารณะ เพื่อจัดการการตั้งค่าทั้งแบบระยะไกลและแบบโลคัลแทนการเข้ารหัสผ่าน

HP Sure Admin ประกอบด้วยส่วนต่าง ๆ ต่อไปนี้:

- **คอมพิวเตอร์ส่วนบุคคลเป้าหมาย:** แพลตฟอร์มที่จะจัดการ ซึ่งรองรับโหมดการรับรองความปลอดภัย BIOS ขั้นสูง
- **HP Manageability Integration Kit (MIK):** ปลั๊กอินสำหรับ System Center Configuration Manager (SCCM) หรือ HP BIOS Configuration Utility (BCU) สำหรับการจัดการการตั้งค่า BIOS จากระยะไกล
- **HP Sure Admin Local Access Authenticator:** แอปโทรศัพท์ที่จะใช้แทนรหัสผ่าน เพื่อให้สามารถเข้าใช้งานการตั้งค่า BIOS แบบโลคัลได้ โดยการสแกนคิวอาร์โค้ดเพื่อรับ PIN แบบใช้ครั้งเดียว

การใช้ HP Sure Admin

เนื้อหาส่วนนี้อธิบายถึงกระบวนการสำหรับการใช้ HP Sure Admin

1. เปิดปลั๊กอิน HP Sure Admin ภายในปลั๊กอิน HP Manageability Integration Kit (MIK) สำหรับ System Configuration Manager (SCCM) หรือ Enhanced BIOS Configuration Utility (BCU)
2. ดาวน์โหลดแอปโทรศัพท์ HP Sure Admin จากร้านค้า Google Play™ หรือ Apple App Store®
3. สร้างคู่มือที่อุปกรณ์เป้าหมายและแอปโทรศัพท์ HP Sure Admin จะใช้ในการรับ PIN แบบใช้ครั้งเดียว เพื่อปลดล็อก BIOS


การปิดใช้งาน HP Sure Admin

หัวข้อนี้อธิบายถึงตัวเลือกในการปิดใช้งาน HP Sure Admin

- ในการตั้งค่า BIOS F10 ให้เลือก **คืนค่าการตั้งค่าความปลอดภัยเป็นค่าเริ่มต้นจากโรงงาน**

 **หมายเหตุ:** คุณจะต้องแสดงตัวตนทางกายภาพ โดยป้อน PIN รับรองความปลอดภัยผ่านแอปโทรศัพท์ HP Sure Admin เพื่อเข้าไปที่การตั้งค่า F10

- ใช้คำสั่ง BCU เพื่อเรียกใช้งาน WMI ของ **คืนค่าการตั้งค่าความปลอดภัยเป็นค่าเริ่มต้นจากโรงงาน** จากระยะไกล

 **หมายเหตุ:** สำหรับข้อมูลเพิ่มเติม โปรดดูคู่มือผู้ใช้ HP BIOS Configuration Utility (BCU)

- ในหน้าการเตรียมด้านความปลอดภัยของ MIK ให้เลือก **ยกเลิกการเตรียม**

2 การสร้างและการจัดการคีย์

ดำเนินการจัดเตรียมระบบความปลอดภัยภายใน MIK ให้เสร็จสมบูรณ์ ก่อนที่จะเปิดใช้งานโหมดการรับรองความถูกต้อง BIOS ขั้นสูง จะต้องเปิดใช้งานโหมดการรับรองความถูกต้อง BIOS ขั้นสูง เพื่อสร้างและส่งออกคีย์ หากต้องการเปิดใช้งานโหมดการรับรองความถูกต้อง BIOS:

- ▲ เปิดปลั๊กอิน HP Sure Admin แล้วเลือก **โหมดการรับรองความถูกต้อง BIOS ขั้นสูง** เพื่อสร้างและส่งออกคีย์


การสร้างและการส่งออกคีย์

มี 3 วิธีในการสร้างคีย์การเข้าใช้งานภายในอุปกรณ์ และเปิดใช้งานแอปโทรศัพท์ HP Sure Admin เพื่อเข้าถึงคีย์

- [สร้างและส่งออกคีย์โดยวิธีการกระจายด้วยตนเองในหน้า 2](#)
- [การสร้างและส่งออกคีย์ด้วย Azure AD Revocation ในหน้า 3](#)
- [สร้างและส่งออกคีย์ไปยัง Azure AD Group OneDrive ในหน้า 4](#)

สร้างและส่งออกคีย์โดยวิธีการกระจายด้วยตนเอง

ใช้ตัวเลือกนี้เพื่อส่งออกคีย์การรับรองความถูกต้องการเข้าใช้งานแบบโลคัล จากนั้นกระจายไปยังแอปโทรศัพท์ HP Sure Admin ด้วยตัวเอง โดยผ่านทางอีเมลหรือวิธีอื่น


 **หมายเหตุ:** ตัวเลือกนี้ไม่ต้องใช้การเข้าถึงเครือข่ายสำหรับแอปโทรศัพท์ HP Sure Admin ในการรับ PIN แบบใช้ครั้งเดียว

1. ตั้งชื่อคีย์ของคุณในช่อง **ชื่อคีย์**
2. ป้อนรหัสผ่านลงในช่อง **รหัสผ่าน**

 **หมายเหตุ:** รหัสผ่านมีไว้เพื่อป้องกันคีย์ที่ส่งออก และจะต้องมีไว้เพื่อให้ผู้ใช้อุปกรณ์ HP Sure Admin สามารถนำคีย์ได้


3. เลือก **เรียกดู** แล้วเลือกตำแหน่งที่จะส่งออกพาร์ในระบบ
4. เลือก **สร้างคีย์** การสร้างคีย์ของคุณจะสำเร็จ เมื่อมีไอคอนแจ้งเตือนปรากฏขึ้นถัดจากปุ่ม **สร้างคีย์** พร้อมข้อความ **สร้างคีย์สำเร็จแล้ว**
5. เลือก **ถัดไป** หน้าสรุปจะแสดงการตั้งค่า HP Sure Admin ที่คุณป้อนไว้
6. เลือก **บันทึกนโยบาย** เมื่อบันทึกนโยบายแล้ว จะมีข้อความ **บันทึกเรียบร้อยแล้ว** ปรากฏขึ้น

7. ไปยังโพลเดอร์ที่คุณบันทึกคีย์ไว้ และกระจายไปยังผู้ใช้แอปโทรศัพท์ HP Sure Admin โดยใช้วิธีที่ผู้ติดตั้งกล่าวสามารถใช้งานบนอุปกรณ์เครื่องนั้นได้ เช่น อีเมล ผู้ใช้รายนี้จะต้องใช้รหัสผ่านในการนำเข้าคีย์ด้วย HP ขอแนะนำให้ใช้กลไกการกระจายที่แตกต่างกัน ระหว่างคีย์และรหัสผ่าน

 **หมายเหตุ:** ในการส่งคิวอาร์โค้ดให้ส่งในขนาดเท่าต้นฉบับ แอปพลิเคชันจะไม่สามารถอ่านรูปภาพได้อย่างถูกต้อง หากมีขนาดเล็กกว่า 800 × 600

การสร้างและส่งออกคีย์ด้วย Azure AD Revocation

ใช้ตัวเลือกนี้เพื่อเชื่อมต่อคีย์การเข้าใช้งานแบบโลคัลกับกลุ่ม Azure Active Directory ที่กำหนด และระบุให้ใช้แอปโทรศัพท์ HP Sure Admin ทั้งในการรับรองความถูกต้องผู้ใช้กับ Azure Active Directory และยืนยันว่าผู้ใช้เป็นสมาชิกของกลุ่มที่กำหนด ก่อนที่จะให้ PIN เข้าใช้งานแบบโลคัล นอกจากนี้ วิธีนี้ยังต้องการการกระจายคีย์การรับรองความถูกต้องการเข้าใช้งานแบบโลคัลไปยังแอปโทรศัพท์ด้วยตัวเอง โดยผ่านทางอีเมลหรือวิธีการอื่น ๆ

 **หมายเหตุ:** ตัวเลือกนี้จะกำหนดให้แอปโทรศัพท์ HP Sure Admin ต้องเข้าใช้งานเครือข่าย เพื่อรับ PIN แบบใช้ครั้งเดียว

1. ตั้งชื่อคีย์ของคุณในช่อง **ชื่อคีย์**
2. ป้อนรหัสผ่านลงในช่อง **รหัสผ่าน**

 **หมายเหตุ:** รหัสผ่านมีไว้เพื่อป้องกันคีย์ที่ส่งออก และจะต้องมีไว้เพื่อให้ผู้ใช้แอปโทรศัพท์ HP Sure Admin สามารถนำคีย์ได้

3. เลือก **เข้าสู่ระบบ Azure AD** แล้วทำการเข้าสู่ระบบ
4. เลือกชื่อกลุ่มของคุณจากกล่องดรอปดาวน์ **ชื่อกลุ่ม Azure AD** คุณต้องเป็นสมาชิกของกลุ่ม จึงจะสามารถเข้าใช้งานคีย์ได้
5. เลือก **เรียกดู** แล้วเลือกตำแหน่งที่จะส่งออกพาดในระบบ
6. เลือก **สร้างคีย์** การสร้างคีย์ของคุณจะสำเร็จ เมื่อมีไอคอนแจ้งเตือนปรากฏขึ้นถัดจากปุ่ม **สร้างคีย์** พร้อมข้อความ **สร้างคีย์สำเร็จแล้ว**
7. เลือก **ถัดไป** หน้าสรุปจะแสดงการตั้งค่า HP Sure Admin ที่คุณป้อนไว้
8. เลือก **บันทึกนโยบาย** เมื่อบันทึกนโยบายแล้ว จะมีข้อความ **บันทึกเรียบร้อยแล้ว** ปรากฏขึ้น
9. ไปยังโพลเดอร์ที่คุณบันทึกคีย์ไว้ และกระจายไปยังผู้ใช้แอปโทรศัพท์ HP Sure Admin โดยใช้วิธีที่ผู้ติดตั้งกล่าวสามารถใช้งานบนอุปกรณ์เครื่องนั้นได้ เช่น อีเมล ผู้ใช้รายนี้จะต้องใช้รหัสผ่านในการนำเข้าคีย์ด้วย HP ขอแนะนำให้ใช้กลไกการกระจายที่แตกต่างกัน ระหว่างคีย์และรหัสผ่าน

 **หมายเหตุ:** ในการส่งคิวอาร์โค้ดให้ส่งในขนาดเท่าต้นฉบับ แอปพลิเคชันจะไม่สามารถอ่านรูปภาพได้อย่างถูกต้อง หากมีขนาดเล็กกว่า 800 × 600


สร้างและส่งคีย์ไปยัง Azure AD Group OneDrive

(แนะนำ) ใช้ตัวเลือกนี้เพื่อหลีกเลี่ยงการแจ้งเตือนการแจ้งเตือนการรับรองความถูกต้องการเข้าใช้งานแบบโลคัลบนโทรศัพท์ เมื่อคุณเลือกตัวเลือกนี้ MIK จะแจ้งเตือนการรับรองความถูกต้องการเข้าใช้งานแบบโลคัลไว้ในโฟลเดอร์ OneDrive ที่กำหนด ซึ่งเข้าใช้งานได้เฉพาะกลุ่มที่อนุญาตเท่านั้น ผู้ใช้แอปโทรศัพท์ HP Sure Admin จะต้องรับรองความถูกต้องกับ Azure AD ในแต่ละครั้งที่จำเป็นต้องใช้ PIN


1. ตั้งชื่อคีย์ของคุณในช่อง **ชื่อคีย์**
2. ป้อนรหัสผ่านลงในช่อง **รหัสผ่าน**
3. เลือก **เข้าสู่ระบบ Azure AD** แล้วทำการเข้าสู่ระบบ
4. เลือกชื่อกลุ่มของคุณจากกล่องดรอปดาวน์ ชื่อกลุ่ม Azure AD

 **หมายเหตุ:** คุณต้องเป็นสมาชิกของกลุ่ม จึงจะสามารถเข้าใช้งานคีย์ได้

5. ป้อนชื่อโฟลเดอร์ OneDrive ที่คุณต้องการใช้บันทึกคีย์ลงในช่อง **OneDrive**
6. เลือก **เรียกดู** แล้วเลือกตำแหน่งที่จะส่งออกพารามิเตอร์ในระบบ
7. เลือก **สร้างคีย์**

 **หมายเหตุ:** การเพิ่มคีย์ของคุณลงในโฟลเดอร์ OneDrive ที่กำหนด และส่งออกไปยังโฟลเดอร์ โลคัลที่ระบุ จะสำเร็จเมื่อมีไอคอนแจ้งเตือนปรากฏขึ้นถัดจากปุ่ม **สร้างคีย์** พร้อมข้อความ **สร้างคีย์เรียบร้อยแล้ว**

8. เลือก **ถัดไป** หน้าสรุปจะแสดงการตั้งค่า HP Sure Admin ที่คุณป้อนไว้
9. เลือก **บันทึกนโยบาย** เมื่อบันทึกนโยบายแล้ว จะมีข้อความ **บันทึกเรียบร้อยแล้ว** ปรากฏขึ้น

 **หมายเหตุ:** ในสถานการณ์นี้ จะไม่จำเป็นต้องส่งข้อมูลใด ๆ ไปยังแอปโทรศัพท์ HP Sure Admin เพื่อทำการจัดเตรียมล่วงหน้า จะมีการจัดเตรียมคอมพิวเตอร์ส่วนบุคคลเป้าหมาย เพื่อให้ชี้ไปยังตำแหน่ง OneDrive ที่อยู่ในคิวอาร์โค้ด แอปโทรศัพท์ HP Sure Admin จะใช้ตัวชี้ในการเข้าถึงตำแหน่ง OneDrive ในกรณีที่ผู้ใช้เป็นส่วนหนึ่งของกลุ่มที่ได้รับอนุญาต และผ่านการรับรองความถูกต้องเรียบร้อยแล้ว

3 การตั้งค่าโทรศัพท์

ดาวน์โหลดแอปโทรศัพท์ HP Sure Admin จาก Google Play หรือ Apple store


- ดาวน์โหลด HP Sure Admin จาก Google store สำหรับโทรศัพท์ Android
- ดาวน์โหลด HP Sure Admin จาก Apple store สำหรับโทรศัพท์ iOS

การใช้แอปโทรศัพท์ HP Sure Admin เพื่อปลดล็อก BIOS

แอปมือถือ HP Sure Admin จะแทนที่การใช้รหัสผ่าน BIOS สำหรับการเข้าใช้งานการตั้งค่า BIOS แบบโวลคัล โดยการป้อน PIN แบบใช้ครั้งเดียว ซึ่งได้รับจากการสแกนคิวอาร์โค้ดที่อยู่บนเครื่องเป้าหมาย

ใช้ขั้นตอนเหล่านี้เพื่อบันทึกคีย์ภายในโทรศัพท์ในสถานการณ์ซึ่งคีย์ดังกล่าวถูกส่งไปยังผู้ใช้แอปโทรศัพท์ในตัวอย่างต่อไปนี้ คีย์ถูกส่งอีเมลไปยังผู้ใช้แอปโทรศัพท์ HP Sure Admin และผู้ใช้จะเปิดอีเมลบนโทรศัพท์

1. เปิดอีเมลที่มีคีย์อยู่
2. เมื่อหน้า **ลงทะเบียน** ปรากฏขึ้น ให้ป้อนรหัสผ่านในช่อง **ป้อนรหัสผ่าน** และป้อนที่อยู่อีเมลของคุณลงในช่อง **ป้อนที่อยู่อีเมลของคุณ** เพื่อถอดรหัสคีย์ และเพิ่มเข้าในแอปพลิเคชัน HP Sure Admin หมายเลข PIN ปลดล็อกจะปรากฏอยู่บนหน้า **PIN ของคุณ**

 **หมายเหตุ:** ขั้นตอนนี้จะทำการบันทึกคีย์ไว้ในอุปกรณ์เคลื่อนที่ และดำเนินการลงทะเบียนให้เสร็จสมบูรณ์ เมื่อถึงขั้นนี้ คุณสามารถใช้แอปโทรศัพท์ HP Sure Admin ในการเข้าใช้งานอุปกรณ์ใด ๆ ก็ตามที่ผ่านการจัดเตรียมให้สามารถเข้าใช้งานด้วยคีย์นี้ได้ จะต้องใช้ที่อยู่อีเมลเฉพาะเมื่อผู้ดูแลระบบกำหนดให้ใช้

3. ป้อน PIN ลงในช่อง **ป้อนรหัสตอบรับของ BIOS**

การขอรับสิทธิ์เข้าถึงการตั้งค่า BIOS หลังการลงทะเบียน

หากต้องการรับสิทธิ์การเข้าใช้งานการตั้งค่า BIOS บนเครื่องเป้าหมายหลังการลงทะเบียน:

1. เข้าสู่การตั้งค่า BIOS ขณะบูทบนเครื่องเป้าหมาย
2. เลือก **สแกนคิวอาร์โค้ด** ในแอปพลิเคชันโทรศัพท์ จากนั้นสแกนคิวอาร์โค้ดบนเครื่องเป้าหมาย
3. หากได้รับข้อความแจ้งให้ทำการรับรองความถูกต้องผู้ใช้ ให้ป้อนข้อมูลประจำตัวของคุณ
4. หมายเลข PIN ที่ปลดล็อกแล้ว จะปรากฏอยู่บนหน้า **PIN ของคุณ**
5. ป้อน PIN ในช่อง **ป้อนรหัสตอบรับของ BIOS** บนเครื่องเป้าหมาย

การปลดล็อก BIOS ด้วย Azure AD Group OneDrive

หากต้องการใช้ HP Sure Admin เพื่อปลดล็อก BIOS ด้วย Azure AD Group OneDrive:

1. เลือก **สแกนคิวอาร์โค้ด** จากนั้นสแกนคิวอาร์โค้ดของ BIOS



หมายเหตุ: แอป HP Sure Admin จะแสดงหน้าเข้าสู่ระบบของ Azure AD

2. เข้าสู่ระบบบัญชีผู้ใช้ Azure ของคุณ

3. ป้อน PIN ลงในช่อง **ป้อนรหัสตอบรับของ BIOS**



หมายเหตุ: แอป HP Sure Admin จะไม่บันทึกคีย์แบบโลคัลในกรณีนี้ แอปโทรศัพท์ HP Sure Admin จะต้องสามารถเข้าใช้งานเครือข่ายได้ และผู้ใช้จะต้องรับรองความถูกต้องในแต่ละครั้งที่จำเป็นต้องใช้ PIN แบบใช้ครั้งเดียว

4 รหัสข้อผิดพลาดของ HP Sure Admin

ใช้ตารางในส่วนนี้เพื่อดูรหัสข้อผิดพลาด ประเภทและคำอธิบายของ HP Sure Admin และคอนโซลผู้ดูแลระบบ KMS

ตาราง 4-1 รหัสข้อผิดพลาด ประเภท และคำอธิบายของแอป HP Sure Admin

| รหัสข้อผิดพลาด | ประเภทข้อผิดพลาด | คำอธิบาย |
|----------------|-----------------------------------|--|
| 100 | QRCodeUnknownError | ข้อผิดพลาดทั่วไป |
| 101 | QRCodeDeserialization | ไม่สามารถอ่าน JSON ของคิวอาร์โค้ด สตรีงเป็นไฟล์ JSON ที่ไม่ถูกต้อง หรือข้อมูลไม่ถูกต้อง |
| 102 | QRCodeInvalidImage | ภาพคิวอาร์โค้ดที่สแกนไม่ถูกต้องไม่สามารถอ่านไฟล์ภาพคิวอาร์โค้ดได้ |
| 103 | QRCodeNoPayload | ภาพคิวอาร์โค้ดที่สแกนไม่ถูกต้องไฟล์ภาพไม่มีส่วนข้อมูล JSON |
| 104 | QRCodeInvalid | ไม่สามารถอ่าน JSON ของคิวอาร์โค้ดได้ สตรีงเป็น JSON ที่ไม่ถูกต้อง หรือข้อมูลในรูปคิวอาร์ไม่ถูกต้อง |
| 105 | QRCodeInvalidKeyIDHash | แฮชคีย์สาธารณะใน JSON ของคิวอาร์โค้ดไม่ตรงกับแฮชคีย์สาธารณะของแพ็คเกจการลงทะเบียน (ข้อมูล KeyID) |
| 106 | QRCodeTampered | รูปภาพคิวอาร์โค้ดที่สแกนถูกแก้ไขและไม่ถูกต้อง |
| 107 | QRCodeTamperedOrInvalidPassPhrase | รูปภาพ QR Code ที่สแกนนั้นถูกแก้ไขและไม่ถูกต้อง หรือวลีรหัสผ่านที่ป้อนไม่ถูกต้อง |

ตาราง 4-2 คีย์การเข้าถึง OneTime จากข้อผิดพลาด ประเภท และคำอธิบายของ OneDrive

| รหัสข้อผิดพลาด | ประเภทข้อผิดพลาด | คำอธิบาย |
|----------------|------------------------------|---|
| 200 | OneTimeKeyError | ข้อผิดพลาดทั่วไป |
| 201 | OneTimeKeyNoUserGroups | ผู้ใช้ที่เข้าสู่ระบบไม่ได้เป็นสมาชิกของกลุ่ม AD ใดๆ ในองค์กรของคุณ |
| 203 | OneTimeKeyInvalidUserGroup | ผู้ใช้ที่เข้าสู่ระบบไม่ได้เป็นสมาชิกของกลุ่ม AD ที่กำหนดสำหรับคีย์นี้ |
| 204 | OneTimeKeyQRFileDoesNotExist | ไม่มีไฟล์คีย์ OneTime ในโฟลเดอร์ OneDrive ของกลุ่ม AD |
| 205 | OneTimeKeyInvalidQRFile | ไฟล์คีย์ OneTime ในโฟลเดอร์ OneDrive ของกลุ่ม AD ไม่ถูกต้อง |
| 206 | OneTimeKeyInvalidQRpayload | มีไฟล์คีย์ OneTime อยู่ แต่ไม่สามารถอ่านส่วนข้อมูลของไฟล์ได้ |

ตาราง 4-3 ข้อผิดพลาดของการรับรองความถูกต้อง Azure AD

| รหัสข้อผิดพลาด | ประเภทข้อผิดพลาด | คำอธิบาย |
|----------------|------------------------------|--|
| 300 | AzureADUnknownError | ข้อผิดพลาดทั่วไป |
| 301 | AzureADInvalidDomain | ที่อยู่อีเมลที่ป้อนไม่ตรงกับชื่อโดเมนที่ระบุในภาพคิวอาร์โค้ด |
| 302 | AzureADAccessToken | เกิดข้อผิดพลาดในการรับโทเค็นการเข้าใช้งานจาก Azure AD ผู้ใช้ไม่สามารถเข้าสู่ระบบ Azure AD สำหรับองค์กรของคุณ หรือแอปไม่มีสิทธิ์ที่จำเป็นในการเชื่อมต่อกับ Azure AD สำหรับองค์กรของคุณ อาจเป็นไปได้ว่าผู้ใช้ได้ยกเลิกการรับรองความถูกต้องแล้ว |
| 303 | AzureADUserProfile | แอป HP Sure Admin ถูกเปิดใช้งานเพื่อรับข้อมูลโปรไฟล์ผู้ใช้จาก Azure AD สำหรับองค์กรของคุณ |
| 304 | AzureADUserPrincipalMismatch | ที่อยู่อีเมลที่ป้อนไม่ตรงกับชื่อหลักของผู้ใช้ที่เข้าสู่ระบบ |
| 305 | AzureADUserInvalidUserGroup | ผู้ใช้ที่เข้าสู่ระบบไม่ได้อยู่ในกลุ่ม Azure AD ที่กำหนดสำหรับคีย์นี้ |

ตาราง 4-4 ข้อผิดพลาด ประเภท และคำอธิบายของคอนโซลผู้ดูแลระบบ KMS

| รหัสข้อผิดพลาด | ประเภทข้อผิดพลาด | คำอธิบาย |
|----------------|----------------------------------|--|
| 401 | KmsUnauthorized | ผู้ใช้ไม่ได้รับอนุญาตให้ใช้บริการ KMS |
| 402 | KmsKeyDoesNotExist | คีย์ส่วนตัวที่ตรงกันไม่มีอยู่ในที่เก็บคีย์ KMS ปัจจุบันคีย์อยู่ในสถานะที่ถูกลบแล้วแต่สามารถกู้คืนได้ และไม่สามารถนำชื่อของคีย์นั้นมาใช้ใหม่ในสถานะนี้ได้ สามารถกู้คืนหรือลบคีย์ได้เท่านั้น |
| 403 | KmsKeyDoesNotExistInTableStorage | ไม่มีคีย์อยู่ในที่จัดเก็บแบบตาราง |
| 404 | KmsUploadKeyErrorInKeyVault | เกิดข้อผิดพลาดขณะเพิ่มคีย์เข้าไปในที่เก็บคีย์ |
| 405 | KmsUploadKeyUnauthorized | ผู้ใช้ไม่ได้รับอนุญาตให้อัปโหลดคีย์ ผู้ใช้ไม่ได้อยู่ในกลุ่ม AD ที่ได้รับอนุญาตซึ่งได้รับอนุญาตให้เรียกใช้ API นี้ |
| 406 | KmsInvalidAzureADLogin | ผู้ใช้ไม่ได้เข้าสู่ระบบใน Azure Tenant AAD |
| 407 | KmsNoUserGroups | ผู้ใช้ที่เข้าสู่ระบบไม่ได้เป็นสมาชิกของกลุ่ม AD ใดๆ ในองค์กรของคุณ |
| 408 | KmsInvalidUserGroup | ผู้ใช้ที่เข้าสู่ระบบไม่ได้เป็นสมาชิกของกลุ่ม AD ที่กำหนดสำหรับคีย์นี้ |
| 409 | KmsInvalidAccessToken | โทเค็นการเข้าถึงที่ระบุไว้ในคำขอไม่ถูกต้อง |
| 410 | KmsAccessTokenExpired | โทเค็นการเข้าถึงที่ระบุหมดอายุแล้ว |
| 411 | KmsAccessTokenInvalidTenantId | โทเค็นการเข้าถึงที่ระบุมีค่า TenantId ที่ไม่ถูกต้อง |

ตาราง 4-4 ข้อผิดพลาด ประเภท และคำอธิบายของคอนโซลผู้ดูแลระบบ KMS (ต่อ)

| รหัสข้อผิดพลาด | ประเภทข้อผิดพลาด | คำอธิบาย |
|----------------|---|--|
| 412 | KmsAccessTokenTenantIdMismatch | TenantId ในโทเค็นการเข้าถึงไม่ตรงกับ TenantId ของแอปที่ใช้งาน |
| 413 | KmsInvalidKeyId | keyId เป็นค่าว่างหรือว่างเปล่า |
| 414 | KmsDeleteKeyUnauthorized | ผู้ใช้ ไม่ได้รับอนุญาตให้ลบคีย์ ผู้ใช้ ไม่ได้อยู่ใน กลุ่ม AD ที่ได้รับอนุญาตซึ่งได้รับอนุญาตให้เรียกใช้ API นี้ |
| 415 | KmsKeyVaultSoftDeleteUnrecoverableState | พยายามที่จะกู้คืนคีย์ล้มเหลวและไม่สามารถกู้คืนได้ ผู้ใช้ควรลองอีกครั้ง |
| 416 | KmsInvalidGetKeysRequest | คำขอ Get Keys ไม่ถูกต้อง |
| 417 | KmsGetKeysUnauthorized | ผู้ใช้ ไม่ได้รับอนุญาตให้ขอรับคีย์ ผู้ใช้ ไม่ได้อยู่ใน กลุ่ม AD ที่ได้รับอนุญาตซึ่งได้รับอนุญาตให้เรียกใช้ API นี้ |
| 418 | KmsInvalidRequestPayload | คำขอที่ได้รับโดย API ไม่ถูกต้อง |
| 419 | KmsRequestRequired | คำขอที่ได้รับต้องไม่ว่างเปล่า |
| 420 | KmsKeyNotConcurrent | คีย์ ในที่เก็บข้อมูลแบบตารางถูกอัปเดตหรือถูก แก่ ไขตั้งแต่ผู้ใช้เรียกสำเนาครั้งสุดท้าย |